Násobíme chytře?

Ľubomíra Balková, Praha, Čeněk Škarda, Uničov

Ačkoliv se na základních školách učíme všichni stejné algoritmy pro sčítání, odčítání, násobení a dělení s tužkou a papírem, je takových algoritmů velké množství a každý z nich má své výhody a nevýhody. Existuje také celá řada mechanických pomůcek, kterými si lidé odedávna výpočty ulehčují. V dnešní době je takovou hlavní pomůckou počítač. I v tomto případě platí, že kromě algoritmů, které používá PC k provádění aritmetických operací, existuje celá řada algoritmů, které se mohou hodit například ve chvíli, kdy je hlavní úlohou násobit obrovská čísla nebo kdy máme k dispozici počítače zapojené do sítí a s výhodou využijeme paralelní algoritmy.

V tomto článku poskytneme přehled více i méně známých algoritmů pro násobení, a to od těch nejstarších, které urychlují násobení zpaměti a s tužkou a papírem, přes mechanismy výpočetních pomůcek až po rychlé algoritmy nejmodernějších počítačů.

1. Násobíme chytře?

Máme-li za úkol vynásobit dvě přirozená čísla a k dispozici tužku a papír, většina z nás použije algoritmus, který jsme se učili na základní škole:

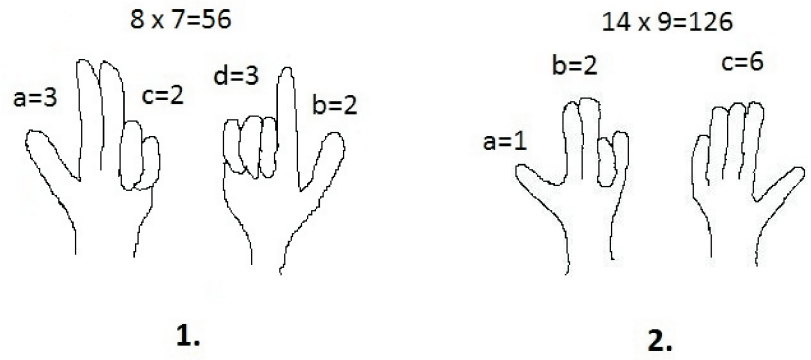
$$\begin{array}{cccc} & & 4 & 7 \\ & \times & 5 & 3 \\ \hline & 1 & 4 & 1 \\ 2 & 3 & 5 & \\ \hline 2 & 4 & 9 & 1 \end{array}$$

Existuje ale celá řada alternativ. *Egyptské a ruské násobení* je založeno na binárním rozvoji násobence. *Cauchyovo komplementární násobení* využívá zápis čísel pomocí záporných cifer. *Čínské násobení* je grafické, a tedy pro žáky s odporem k matematice možná nejpřívětivější. Zjednodušení násobení velkých čísel přinesly *tabulky kvadrátů* a *Napierovy kosti*, vynález Johna Napiera, otce logaritmu. Kromě algoritmů, které urychlují násobení zpaměti a na papíře, si také ukážeme efektivní algoritmy pro počítačové násobení. Při násobení velkých čísel se vyplatí zapsat čísla v tzv. *redundantní binární soustavě*, kde je dovolena kromě cifer 0 a 1 i cifra -1. Moderní éru násobení velkých čísel odstartoval ale zejména *Karacubův algoritmus*, který taktéž v krátkosti představíme.

Ing. Ľubomíra Balková, Ph.D., Katedra matematiky FJFI ČVUT v Praze, Trojanova 13, 120 00 Praha 2, e-mail: lubomira.balkova@fjfi.cvut.cz, Čeněk Škarda, Gymnázium Uničov, Gymnazijní 257, 783 91 Uničov, e-mail: Cenek.Skarda@seznam.cz

2. Násobení zpaměti

Násobení na prstech paní učitelky na základní škole nevidí rády. Chtějí nás totiž naučit násobit do 10 krát 10 zpaměti „jako když bičem mrská“. Přesto je použití prstů přirozeným zjednodušením, kterým si lidé pomáhají při výpočtech odedávna. Středověcí obchodníci s oblibou využívali tzv. *cikánskou násobilku*, která umožňuje násobit pomocí prstů do 9 krát 9 (se znalostí pouhé násobilky do 5 krát 5). Princip cikánské násobilky pochopíte z obrázku 1. Pokud chceme násobit 8 krát 7, zeptáme



Obr. 1. **1.** Cikánská násobilka pro výpočet 8×7 **2.** Výpočet 14×9 pomocí prstů

se: „Osm a kolik je deset?“ „A dva.“ Skrčíme dva prsty na první ruce ($c = 2$). To samé uděláme s číslem sedm. Schováme tedy tři prsty na druhé ruce ($d = 3$). Na pozici desítek napíšeme součet vztyčených prstů ($a + b = 3 + 2 = 5$) a na pozici jednotek napíšeme součin skrčených prstů ($c \times d = 2 \times 3 = 6$). A obdržíme správný výsledek 56. Bystrý čtenář si snadno rozmyslí, že algoritmus je použitelný jen k násobení čísel, která jsou obě větší nebo rovna 5, a že funguje díky následujícím rovnostem

$$\begin{aligned}(10-c)(10-d) &= 100-(c+d)10+cd,\\ &= 10(10-c-d)+cd,\\ &= 10(a+b)+cd.\end{aligned}$$

Možná už čtenář postřehl, že při násobení některých čísel narazíme na úskalí. Například při násobení 7×6 je $c \times d = 3 \times 4 = 12$, což je více než 10. V takovém případě na místě jednotek necháme číslo 2 a 1 přeneseme k desítkám.

Násobení devíti nedělalo středověkým trhovcům problémy ani pro násobence od 12 do 19. Jejich postup naznačuje obrázek 1. Pokud chceme násobit 14 krát 9, skrčíme na levé ruce čtvrtý prst – prsteníček. Zleva pak první prst – palec – reprezentuje stovky ($a = 1$), zbylé prsty před skrčeným reprezentují desítky ($b = 2$) a prsty, které následují za skrčeným, reprezentují jednotky ($c = 6$). Výsledek: 126. Snadno si rozmyslíme, že algoritmus funguje díky následujícím rovnostem. Násobíme-li $(10 + d)$ krát 9, kde $d = 2, \ldots, 9$, platí:

$$\begin{aligned}(10+d)9 &= 90+9d,\\ &= 100+10(d-2)+(10-d),\\ &= 100a+10b+c.\end{aligned}$$

3. Násobení s tužkou a papírem

3.1. Egyptské násobení

Toto násobení je založeno na binárním zápisu násobence, viz [8]. Chceme-li egyptským způsobem vynásobit např. 13 krát 15, sestavíme si tabulku, jejíž první sloupec tvoří mocniny dvou menší nebo rovné 13 a druhý sloupec vznikne postupným zdvojováním 15. V prvním sloupci si zaškrtneme mocniny dvou, které se vyskytují v binárním zápisu 13. Binární zápis lze získat hladovým algoritmem: Podíváme se, jakou nejvyšší mocninu dvojky číslo 13 obsahuje. To je 8. Poté od 13 odečteme 8 a pro získaný rozdíl 5 opět najdeme největší mocninu dvojky, kterou číslo 5 obsahuje. To je 4. Na závěr vypočíteme rozdíl $5 - 4 = 1$, a to je nultá mocnina dvojky. Získáme $13 = 1 + 4 + 8$. Pak již stačí sečíst ve druhém sloupci řádky odpovídající podtrženým mocninám dvou. Výsledek: 195. Všimněte si, že se obejdeme bez malé násobilky. Stačí umět zdvojovat a hledat binární rozvoj.

13	×	15
$\underline{1}$		15
2		30
$\underline{4}$		60
$\underline{8}$		120
		195

Obr. 2. Výpočet 13×15 egyptským (etiopským) způsobem

A odkud Egypťané věděli, že každé číslo má binární zápis, tj. může být vyjádřeno jako součet mocnin dvou? Pravděpodobně díky rovnoramenným vahám. Ty totiž používali a mohli si tedy všimnout, že mají-li závaží hmotnosti n debenů (základní jednotka staroegyptského systému měření hmotnosti), mohou si pomocí rovnoramenných vah vyrobit závaží hmotnosti $2n$ debenů tak, že na jednu misku vah položí n-debenové závaží a na druhé misce vah jej vyváží. Spojením použitých předmětů vznikne hledané závaží hmotnosti $2n$ debenů. Poté již stačilo vypozorovat, že každý předmět hmotnosti m krát n debenů, kde m je přirozené číslo, je možno vyvážit pomocí závaží o hmotnostech $n, 2n, 4n, 8n$ atd.

3.2. Ruské (sedlácké) násobení

Ruské násobení se velmi podobá egyptskému. Ještě v 19. století se používalo na ruském venkově a zřejmě tak násobila většina Evropanů před prosazením indo-arabského způsobu násobení, který se dnes učíme na základní škole.

Chceme-li ruským způsobem vynásobit 13 krát 15, sestavíme si tabulku, jejíž první sloupec tvoří zbytky po opakovaném celočíselném dělení násobence dvojkou a druhý sloupec vznikne postupným zdvojováním 15. Nyní stačí sečíst ve druhém sloupci řádky odpovídající jednotkovým zbytkům. Výsledek: 195.

Uvědomte si, že pokud přirozené číslo n není dělitelné dvojkou, znamená to, že na posledním místě v jeho binárním zápisu je jednička. Pokud je dělitelné dvojkou, pak má v binárním zápisu na posledním místě nulu. Snadno si pak rozmyslíte, že binární zápis čísla n lze získat také následujícím algoritmem:

1. Vyděl číslo dvěma.
2. Je-li dělitelné, zapamatuj si nulu a číslo $n/2$. Není-li dělitelné, zapamatuj si jedničku a číslo $(n-1)/2$.
3. Pokud zapamatované číslo není nula, opakuj algoritmus. Pokud zapamatované číslo je nula, binární zápis získáš sepsáním nul a jedniček zleva doprava v pořadí od poslední zapamatované cifry k první.

13	×	15
$13 : 2 = 6$	zbytek 1	15
$6 : 2 = 3$	zbytek 0	30
$3 : 2 = 1$	zbytek 1	60
$1 : 2 = 0$	zbytek 1	120
		195

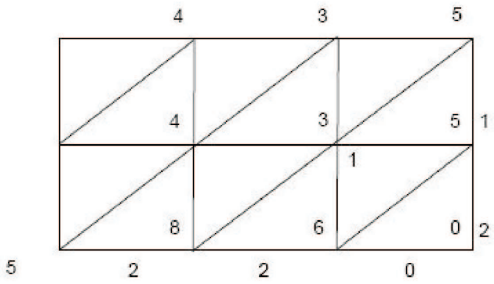
Obr. 3. Výpočet 13×15 ruským způsobem

3.3. Indické násobení

Zde popsané násobení není jediné, které se ve staré Indii používalo. Existovalo více než osm rozličných způsobů násobení, které se však v principu velmi podobaly, viz [7].

Chceme-li indickým způsobem vynásobit 435 krát 12, namalujeme tabulku se třemi sloupci a dvěma řádky, které označíme ciframi násobence a násobitele, a každé okénko tabulky rozdělíme úhlopříčkou na dva trojúhelníky. Nyní tabulku vyplníme tak, že pro každou buňku násobíme cifry, kterými jsou označeny řádek a sloupec, v nichž se buňka nachází. Pokud vyjde číslo menší než deset, napíšeme je do dolního trojúhelníku. Pokud je výsledek větší nebo roven deseti, napíšeme desítky do horního trojúhelníku a jednotky do dolního trojúhelníku.

Na závěr vysčítáme zprava doleva čísla podél úhlopříček. Jednotky sepisujeme a desítky si pamatujeme a „přenášíme“ je. Výsledek: 5 220.



Obr. 4. Výpočet 435×12 indickým způsobem

3.4. Al-Chwárizmího násobení

Násobení si ukážeme na příkladu 23 123 krát 2 131. Nejdříve si napíšeme násobence a pod něj násobitele tak, aby jednotky násobitele byly pod nejvyšší cifrou násobence.

			$\underline{2}$	3	1	2	3
2	1	3	1				
4	2	6	2|	$\underline{3}$	1	2	3
	2	1	3	1			
4	9	0	1	3|	$\underline{1}$	2	3
		2	1	3	1		
4	9	2	2	6	1|	$\underline{2}$	3
			2	1	3	1	
4	9	2	6	8	7	2|	$\underline{3}$
				2	1	3	1
4	**9**	**2**	**7**	**5**	**1**	**1**	**3**

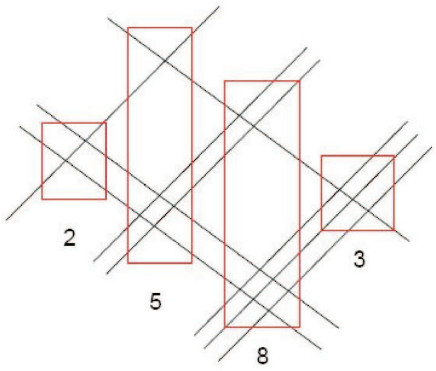
Poté vezmeme nejvyšší cifru násobence (v našem případě 2) a vynásobíme násobitele. Tím dostaneme číslo 4 262, které napíšeme před násobence tak, že jednotkovou cifrou nahradíme nejvyšší cifru násobence. Pak násobitele posuneme o jednu cifru doprava. Další násobení provedeme číslem 3, vyjde nám 6 393 a toto číslo přičteme k částečnému výsledku 4 262 tak, že poslední cifrou přepíšeme trojku. Násobitele posuneme o jednu cifru doprava. Další budeme podobně násobit jedničkou a znovu výsledek přičteme tak, že poslední cifra nahradí jedničku. Násobitele opět posuneme o jednu cifru doprava a provedeme násobení totožně i se zbylými ciframi násobence. Nakonec nám vyjde číslo 49 275 113, což je výsledek násobení čísel 23 123 a 2 131 ([1], str. 190–191).

Al-Chwárizmí byl matematik arabského původu žijící okolo let 780–850. Z jeho díla se dochovalo pět částečně přepracovaných opisů, které jsou věnovány algebře, astronomii, geografii a výpočtům kalendáře. Jeho práce v oblasti aritmetiky a algebry měly velký vliv na další rozvoj matematiky. Části jeho práce byly později přebírány a komentovány v pracích následujících desítek generací. Al-Chwárizmího aritmetický traktát je první známou arabskou prací, v níž je vyložena indická desítková poziční soustava a objasněny matematické úkony v této soustavě. Tato jeho práce se dochovala pouze v jediném latinském překladu z poloviny 13. století, který však není plně dokončený a začíná slovy: „Algorizmi pravil...“. Právě z této zkomoleniny Al-Chwárizmího jména pochází slovo algoritmus. Z Al-Chwárizmího algebraického traktátu zase pochází slovo al-džebr, v němž má původ dnešní termín algebra, který označoval sečtení dvou rovnic s cílem zbavit se neznámé. Další latinské spisy jako např. *Algorizmova kniha o praxi aritmetiky* (1135–1153) nebo *Kniha uvedení Algorizma do umění astronomického, sestavená mistrem A.* (kolem r. 1143) se částečně odvolávají na Al-Chwárizmího a jeho díla.

3.5. Čínské grafické násobení

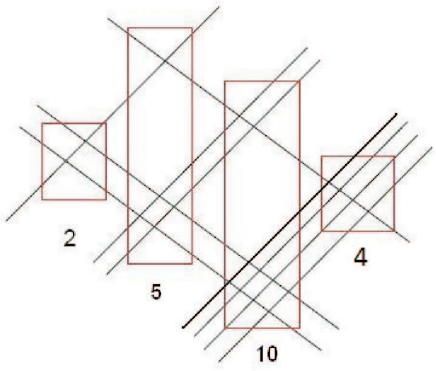
Čínské grafické násobení se nejspíše vyvinulo díky lásce Číňanů ke kaligrafii a malbě a jejím následným uplatněním v matematice při násobení menších čísel.

Chceme-li tímto způsobem vynásobit 123 krát 21, namalujeme za násobence ve směru z JZ na SV postupně jednu rovnoběžku za stovky, dvě rovnoběžky za desítky a tři rovnoběžky za jednotky, viz obrázek 5. Poté za násobitele namalujeme ze SZ směrem na JV dvě rovnoběžky za desítky a jednu za jednotky. Poté do disjunktních obdélníků uzavřeme průsečíky odpovídající tisícům, stovkám, desítkám a jednotkám a zjistíme jejich počty. V našem případě máme v prvním obdélníku 2 průsečíky, ve



Obr. 5. Výpočet 123×21 čínským grafickým způsobem

druhém 5, ve třetím 8 a ve čtvrtém 3. Výsledek: 2 583. Tímto způsobem bychom postupovali i při násobení větších čísel. Pokud by nám součet průsečíků v některém obdélníku vyšel větší než 9, přičetli bychom cifru desítek k následujícímu obdélníku. Ilustrujme tuto situaci pro 124 krát 21, viz obrázek 6. Nyní nám vyšlo v prvním



Obr. 6. Výpočet 124×21 čínským grafickým způsobem

odélníku 2, ve druhém 5, ve třetím 10 (jedničku přičteme k druhému obdélníku) a ve čtvrtém 4. Výsledek je tedy 2 604.

3.6. Cauchyovo komplementární násobení

Toto násobení využívá zápis čísel pomocí záporných cifer. Všimněme si, že při použití Cauchyova komplementárního násobení si vystačíme s násobilkou do 5 krát 5.

Chceme-li násobit 57 krát 17 Cauchyovým algoritmem, zapíšeme nejprve násobence i násobitele pomocí cifer od -4 do 5, tj. $57 = 1\overline{43} = 100 - 40 - 3$ a $17 = 2\overline{3} = 20 - 3$. Pruhy nad ciframi znamenají, že cifry mají znaménko mínus. Poté již násobíme analogicky jako v klasické desítkové soustavě, viz obrázek 7. Pouze u znamének dáváme

	1	$\overline{4}$	$\overline{3}$
	$\times$	2	$\overline{3}$
	-2	2	9
2	-8	-6	
1	0	-4	9
	9	6	9

Obr. 7. Výpočet 57×17 Cauchyovým algoritmem

pozor: při násobení dvou záporných cifer nebo dvou kladných cifer má výsledek znaménko plus, při násobení cifer opačného znaménka má výsledek znaménko mínus. Abychom mohli Cauchyovo komplementární násobení používat, musíme umět převádět zápisy čísel mezi klasickou desítkovou soustavou a desítkovou soustavou s ciframi od -4 do 5. K takové konverzi slouží následující jednoduchý algoritmus:

1. Chceme-li zapsat 57 v desítkové soustavě s ciframi od -4 do 5, v prvním kroku přičteme 44 (obecně přičteme číslo sestavené z tolika čtyřek, kolik cifer má číslo konvertované)
$$57 + 44 = 101.$$
Poté odečteme od posledních dvou cifer (obecně tolika, kolik cifer má číslo konvertované) součtu číslo 4
$$0 - 4 = -4 \quad \text{a} \quad 1 - 4 = -3.$$
Výsledek: $1\overline{43}$.
2. Chceme-li naopak zapsat $1\overline{43}$ v klasické desítkové soustavě, vypočíteme rozdíl kladné a záporné části:
$$100 - 43 = 57.$$
Výsledek: 57.

4. Násobení pomocí tabulek a mechanických pomůcek

4.1. Tabulky kvadrátů

Už staří Babyloňané znali vzorce:

$$ab = \frac{1}{2}\left((a+b)^2 - a^2 - b^2\right),$$

$$ab = \frac{1}{4}\left((a+b)^2 - (a-b)^2\right).$$

V roce 1690 uvádí Johann Hiob Ludolf ve svém díle *Tetragonometrie* návod, jak pomocí tabulek kvadrátů násobit přirozená čísla. Všimněte si, že právě z babylonských vzorců je zřejmé, že pro výpočet součinu jakýchkoliv přirozených čísel stačí mít k dispozici dost velkou tabulku kvadrátů přirozených čísel. V roce 1817 Antoine Voisin vydává první takové multiplikační tabulky. A poté v roce 1833 vycházejí Kulikovy tabulky násobení a tabulky kvadrátů, které necitují Ludolfa a Voisina, protože Jakub Filip Kulik o práci svých předchůdců zřejmě nevěděl. Kulik vytvořil tabulky součinů dvojciferných přirozených čísel. Násobení přirozených čísel se pak díky nim zjednodušilo na pouhé sčítání, viz následující ilustrace. Chceme-li násobit 1743 krát 37, stačí najít v tabulce součin 43×37 a 17×37 a výsledky správně sečíst.

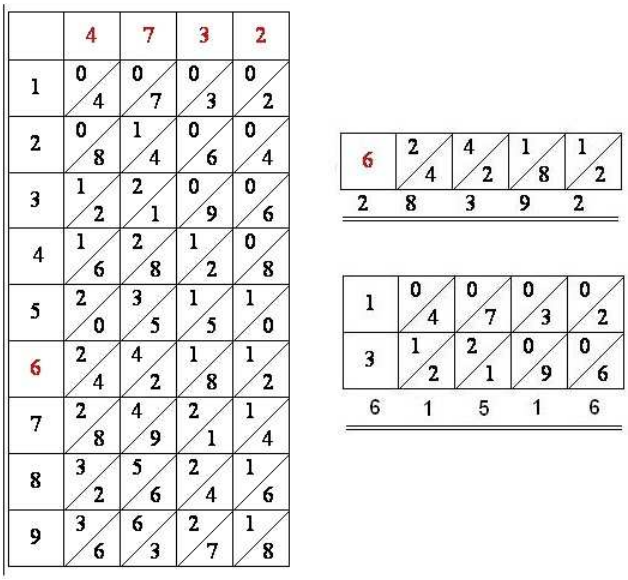
$$\begin{array}{rcrcrrrrr} 43 & \times & 37 & = & & 1 & 5 & 9 & 1 \\ 17 & \times & 37 & = & 6 & 2 & 9 & & \\ \hline & & & & 6 & 4 & 4 & 9 & 1 \end{array}$$

Jelikož je Kulikovo jméno v dějinách české matematiky významné, řekneme si o něm alespoň pár základních informací. **Jakub Filip Kulik** (1793–1863) se narodil ve Lvově a jeho hrobku najdeme na vyšehradském Slavíně [5]. Studoval filozofii a práva na tamní univerzitě, brzy však začal tíhnout k matematice. V roce 1814 se přihlásil do konkurzu na místo profesora olomouckého lycea a téhož roku tam byl jmenován řádným profesorem. O dva roky později byl jmenován profesorem fyziky na univerzitě ve Štýrském Hradci. Na této univerzitě složil roku 1822 doktorské zkoušky a o rok později byl zvolen jejím rektorem. V roce 1826 byl jmenován profesorem vyšší matematiky na univerzitě v Praze. Vedle podrobných učebnic vyšší analýzy a mechaniky jsou nejvýznamnější jeho díla tabulková (tabulky násobení, druhých a třetích mocnin, logaritmické, trigonometrických a hyperbolických funkcí a jejich logaritmů, tabulky k výpočtu obsahu válcových a kuželových nádob, dělitelů čísel, primitivních kořenů). Kromě toho Kulik sestavil známé Kulikovy tabulky dělitelů čísel od 3 do 100 milionů, které byly uloženy do knihovny vídeňské císařské akademie věd a na kterých Kulik pracoval dvacet let. Poznamenejme, že při ručním sestavování tak obsáhlých tabulek se Kulik samozřejmě nevyhnul chybám. Navíc v dnešní době počítačů jeho dílo přirozeně upadlo v zapomnění.

4.2. Napierovy kosti

Tyto výpočetní pomůcky byly vyrobeny ze slonoviny, odtud jejich název, neboť připomínaly svou barvou a tvarem kosti. Vymyslel je skotský matematik John Napier na sklonku svého života. Pomocí nich můžeme jednoduše převést násobení a dělení na sčítání. Základní kostky se skládají z devíti samostatných sloupků, rozdělených na deset řádků. V prvním řádku je vždy uvedeno číslo 1 až 9 a v následujících devíti jsou vzestupně uvedeny jeho násobky čísly 1 až 9.

Násobení si vysvětlíme na příkladu 4 732 krát 6. Z Napierových kostí si vezmeme sloupky odpovídající cifrám násobence a seřadíme je tak, aby nám vzniklo žádané číslo (v našem případě číslo 4 732). Poté si najdeme řádek odpovídající násobiteli (v našem případě řádek 6). Nyní již pouze sečteme čísla v horních a dolních částech tohoto řádku a to tak, že je vždy sčítáme po diagonále, viz obrázek 8. Všimněme si podobnosti s indickým násobením.



Obr. 8. Výpočet 4732×6 a 4732×13 pomocí Napierových kostí

John Napier of Merchiston (1550–1617) byl skotský matematik, fyzik, astronom a astrolog. Do paměti se zapsal jako vynálezce logaritmu, proto se na jeho počest přirozenému logaritmu (tedy logaritmu o základu e) říká Napierův logaritmus. Dále je Napier autorem desetinného zápisu zlomků a jednoho z prvních mechanických kalkulátorů. Ve svém článku *Rabdologiae* o násobení navrhuje totiž mechanismus stroje pro násobení a dělení velkých čísel.

5. Počítačové násobení

Násobení v binární soustavě a redundantní binární soustavě není pro člověka běžné. Lidé totiž díky deseti prstům provádějí výpočty v soustavě desítkové, tj. čísla zapisují pomocí mocnin desítky a cifer od 0 do 9. Se soustavou binární ovšem pracuje valná většina počítačů. Každé přirozené číslo n lze právě jedním způsobem vyjádřit ve tvaru: $n = a_k 2^k + a_{k-1} 2^{k-1} + \cdots + a_1 2^1 + a_0 2^0$, kde koeficienty $a_k, a_{k-1}, \ldots, a_1, a_0$ nabývají hodnot nula nebo jedna a $a_k = 1$. Řetězci $a_k a_{k-1} \ldots a_1 a_0$ říkáme binární zápis čísla n. Připomeňme, že binární zápis se získá hladovým algoritmem, viz kap. 3.1. o egyptském násobení. Například $13 = 2^3 + 2^2 + 2^0$, proto 13 má v binární soustavě zápis 1101. Násobení v binární soustavě je velmi podobné nám známému klasickému násobení v desítkové soustavě. Například číslo 11 s binárním zápisem 1011 a číslo 5 s binárním zápisem 101 se vynásobí následujícím způsobem.

$$\begin{array}{cccccc} & & 1 & 0 & 1 & 1 \\ & & \times & 1 & 0 & 1 \\ \hline & & 1 & 0 & 1 & 1 \\ & 0 & 0 & 0 & 0 & \\ 1 & 0 & 1 & 1 & & \\ \hline 1 & 1 & 0 & 1 & 1 & 1 \end{array}$$

Výsledek je $32+16+4+2+1=55$. Všimněte si, že rychlost násobení odpovídá počtu jedniček v binárním zápisu násobitele (v našem případě jsou dvě jedničky v binárním zápisu 5), právě tolik sčítání $(n+k-1)$-bitových čísel, kde n je počet bitů násobence a k počet bitů násobitele, totiž musíme provést.

5.1. Redundantní binární soustava

Připusťme nyní v binární soustavě cifry $-1, 0$ a 1. Zápisy čísel už nejsou jediné možné, soustava je redundantní. Například $15 = 8+4+2+1$ a také $15 = 16-1$, tedy jak 1111, tak i $1000\overline{1}$ jsou zápisy 15 v redundantní binární soustavě. Vyberme zápis s maximálním počtem nul. K tomu stačí aplikovat následující přepisovací pravidla, dokud je co přepisovat:

$$\begin{aligned} 01111 &\to 1000\overline{1},\\ 0\overline{1}\overline{1}\overline{1}\overline{1} &\to \overline{1}0001,\\ 1\overline{1} &\to 01,\\ \overline{1}1 &\to 0\overline{1}. \end{aligned}$$

Zatímco průměrný počet nul ve standardním binárním zápisu je $1/2$, v redundantním binárním zápisu s maximálním možným počtem nul jsou to $2/3$. Jelikož je rychlost násobení úměrná počtu nul, je jasné, že redundantní binární soustava je pro násobení velkých čísel výhodnější. Poznamenejme ještě, že násobíme analogicky jako v klasické binární soustavě. Pouze u znamének dáváme pozor: při násobení cifer stejného znaménka má výsledek znaménko plus, při násobení cifer opačného znaménka má výsledek znaménko mínus. Tedy například násobení 11 a 5 proběhne následovně:

$$\begin{array}{cccccccc} & & 1 & 0 & \overline{1} & 0 & \overline{1} \\ & & & \times & 1 & 0 & 1 \\ \hline & & 1 & 0 & \overline{1} & 0 & \overline{1} \\ & 0 & 0 & 0 & 0 & 0 & \\ 1 & 0 & \overline{1} & 0 & \overline{1} & & \\ \hline 1 & 0 & 0 & \overline{1} & 0 & 0 & \overline{1} \end{array}$$

Výsledek je tedy $64-8-1=55$.

5.2. Rychlé násobení

Rychlé násobení je násobení se složitostí menší, než má násobení klasické, jehož složitost je $\mathcal{O}(n^2)$, kde n je délka binárního zápisu většího čísla z násobence a násobitele. Znamená to existenci takové konstanty $C>0$, že pro vynásobení dvou čísel s délkou binárního zápisu maximálně n je potřeba provést maximálně $C\cdot n^2$ binárních operací. Snaha o zrychlení algoritmů se zesiluje ruku v ruce s rozvojem počítačů a speciálně snaha o maximální zrychlení násobení je dána potřebami kryptografie, kde je nutné násobit v přijatelném čase ohromná čísla (řádově 10^{100}). My zde popíšeme jediné z rychlých násobení – *Karacubovo násobení* založené na důvtipné myšlence a poměrně jednoduše vysvětlitelné. Mezi rychlými algoritmy patří k těm nejstarším, ovšem algoritmy ještě rychlejší už jsou příliš technické. Zájemce o násobení přirozených čísel s binárním rozvojem délky n blížící se svou složitostí libovolně blízko až k nejnižší

hranici $\mathcal{O}(n)$ si dohledá podrobnosti v knize [4]. Poznamenejme, že jde o jednu z nejrespektovanějších publikací v oboru programování. Její autor Donald E. Knuth je průkopníkem oboru matematické analýzy algoritmů a významnou osobností v mnoha dalších oborech teoretické počítačové vědy.

Karacubovo násobení vyvrátilo domněnku, že složitost násobení dvou přirozených čísel s binárním rozvojem délky n je $\mathcal{O}(n^2)$. Tento názor razil ještě v roce 1960 na semináři moskevské univerzity zakladatel teorie složitosti algoritmů Andrej N. Kolmogorov. Semináře se účastnil i jeho student Anatolij A. Karacuba, který navrhl důvtipný algoritmus s nižší složitostí [2, 3]. Popíšeme algoritmus, který je založen na stejné myšlence jako původní Karacubův, ale je ještě trochu jednodušší. Chceme násobit dvě $2n$-bitová čísla U s binárním zápisem $u_{2n-1}\dots u_1u_0$ a V s binárním zápisem $v_{2n-1}\dots v_1v_0$. Zapíšeme U, V následujícím způsobem $U = 2^nU_1 + U_0$ a $V = 2^nV_1 + V_0$. Platí tedy, že U_1 má binární zápis $u_{2n-1}\dots u_n$ a U_0 má zápis $u_{n-1}\dots u_1u_0$, podobně V_1 má binární zápis $v_{2n-1}\dots v_n$ a V_0 má zápis $v_{n-1}\dots v_1v_0$. Následující formule redukuje problém na 3 násobení n-bitových čísel, několik sčítání, resp. odečítání a posouvání binární čárky: $U \times V = (2^{2n} + 2^n)U_1V_1 + 2^n(U_1 - U_0)(V_0 - V_1) + (2^n + 1)U_0V_0$. Ilustrujme Karacubův algoritmus pro $U \times V$, kde $U = 210$ a $V = 119$. Binární zápis U je 11010010 a binární zápis V je 01110111.

$$210 = U = 2^4U_1 + U_0 = 2^4 \cdot 13 + 2,$$

$$119 = V = 2^4V_1 + V_0 = 2^4 \cdot 7 + 7,$$

kde $U_1 = 13$ má binární zápis 1101 a $U_0 = 2$ má binární zápis 0010, $V_1 = V_0 = 7$ mají zápis 0111.
Nyní určíme 3 součiny nejvýše 4-bitových čísel: U_1V_1, $(U_1 - U_0)(V_0 - V_1)$, U_0V_0. V tomto konkrétním případě je $V_0 = V_1$, a tedy prostřední součin je nulový.

U_1V_1 :

			1	1	0	1	
			×	1	1	1	
			1	1	0	1	
		1	1	0	1		
	1	1	0	1			
1	0	1	1	0	1	1	

U_0V_0 :

	1	1	1
	×	1	0
1	1	1	0

Na závěr zbývá provést násobení 2^8 a 2^4, což je vlastně připsání 8, respektive 4 nul na konec binárního zápisu původního čísla, a sčítání.

$$U \times V = 2^8U_1V_1 + 2^4U_1V_1 + 2^4U_0V_0 + U_0V_0.$$

$U \times V$:

1	0	1	1	0	1	1	0	0	0	0	0	0	0	0	0
				1	0	1	1	0	1	1	0	0	0	0	0
							1	1	1	0	0	0	0	0	0
											1	1	1	0	
1	1	0	0	0	0	1	1	0	0	1	1	1	1	0	

Po konverzi do desítkové soustavy máme správný výsledek

$$210 \times 119 = 2^{14} + 2^{13} + 2^8 + 2^7 + 2^4 + 2^3 + 2^2 + 2^1 = 24\,990.$$

Není těžké dokázat, že složitost Karacubova násobení je $\mathcal{O}(n^{\log_2 3})$. Číslo $\log_2 3$ je přibližně rovno $1,585$, což je číslo menší než 2, a tedy jde skutečně o rychlé násobení podle naší definice. Adaptací na desítkovou soustavu lze převést násobení 8-místných čísel na násobení čísel 4-místných, které už dobří počtáři zvládnou zpaměti. Nezdá se však, že by takovou metodu používali „zázračníˇ počtáři“, kteří v minulosti bavili obecenstvo násobením obrovských čísel zpaměti.

Poznamenejme pro úplnost, že nejrychlejším v praxi používaným algoritmem je Schönhageův–Strassenův algoritmus se složitostí $\mathcal{O}(n \log n \log\log n)$ z roku 1971, ale existují i algoritmy, které jsou asymptoticky ještě rychlejší (např. Fürerův algoritmus z roku 2007 nebo algoritmus autorů De, Saha, Kurur a Saptharishi z roku 2008).

6. Závěr

Cílem tohoto článku bylo ukázat, že algoritmů násobení existuje celá řada a že ty z nich, které se všichni učíme na základních školách, nejsou občas nejvýhodnější. Autoři zároveň vytvořili www stránku `http://bimbo.fjfi.cvut.cz/~soc`, která nejrůznější algoritmy srozumitelně popisuje a ilustruje na příkladech či pomocí programů.

Poděkování. Autoři děkují za cenné připomínky RNDr. Pavle Pavlíkové, Ph.D., a doc. RNDr. Martinu Klazarovi, Dr.

Literatura

[1] Juškevič, A. P.: *Dějiny matematiky ve středověku*, 1.vydání. Academia, Praha 1978.

[2] Karacuba, A. A., Ofman, Yu.: *Multiplication of many-digital numbers by automatic computers* (v ruštině). Proc. of the USSR Academy of Sciences *145* (1962), 293–294.

[3] Karacuba, A. A.: *The complexity of computation* (v angličtině). Proc. Steklov Inst. Math. *211* (1995), 169–183.

[4] Knuth, D. E.: *The art of computer programming volume 2: Seminumerical algorithms*, 3rd ed. Addison-Wesley, Boston, 1998.

[5] Křížek, M., Šolcová, A.: *Procházky Prahou matematickou, fyzikální a astronomickou (3. část)*. PMFA *55* (3) (2010), 215–230.

[6] Porubský, Š.: *Ako rýchlo vieme a možeme násobiť*. Sborník 30. mezinárodní konference Historie matematiky, J. Bečvář, M. Bečvářová, (eds), Matfyzpress, 2009.

[7] Sýkorová, I.: *Násobení ve středověké Indii*. Sborník 29. mezinárodní konference Historie matematiky, J. Bečvář, M. Bečvářová, (eds), Matfyzpress, 2008.

[8] Vymazalová, H.: *Staroegyptská matematika*. Dějiny matematiky, svazek 31, Praha 2006.

[9] Biografie českých matematiků, `inserv.math.muni.cz/biografie`